TOM DAVIS, VIRGINIA
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

Majority (202) 225–5074
Minority (202) 225–5051

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
Fax: 202 225-2382

Statement of Rep. Christopher Shays
March 2, 2005

The Cold War cult of secrecy remains largely impervious to the new security imperatives of the post-9/11 world. Overclassification is a direct threat to national security.

Last year, more federal officials classified more information, and declassified less, than the year before. In our previous hearing on official secrecy policies, the Department of Defense (DOD) witness estimated that fully half of all the data deemed "Confidential," "Secret" or "Top Secret" by the Pentagon was needlessly or improperly withheld from public view. Further resisting the call to move from a "need to know" to a "need to share" standard, some agencies have become proliferators of new categories of shielded data. Legally ambiguous markings like "Sensitive but Unclassified", "Sensitive Homeland Security Information" and "For Official Use Only" create new bureaucratic barriers to information sharing. These pseudo-classifications can have persistent and pernicious practical effects on the flow of threat information.

The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) concluded that, "Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs… are substantial."

Those costs are measured in lives as well as dollars. Somewhere in the vast cache of data that never should have been classified, and may never be declassified, is that tiny nugget of information that, if shared, could be used to detect and prevent the next deadly terrorist attack.

Recently enacted reforms should help focus and coordinate disparate elements of the so-called "intelligence community" to broaden our view of critical threat information. The previously ignored, and still unfunded, Public Interest Declassification Board has new authority to push for executive branch adherence to disclosure standards, particularly with regard to congressional committee requests.

But those promising initiatives still confront deeply entrenched habits and cultures of excessive secrecy. The 9/11 Commission successfully worked through security barriers to access and publish the information they needed. But as soon as the Commission's legal mandate expired, heavy-handed classification practices reasserted themselves. As a result, release of the final staff report on threats to civil aviation was delayed. And the version finally made public contains numerous redactions, some of which needlessly seek to shield information already released by other agencies.

The Cold War was a struggle of the Industrial Age. The global war against terrorism is being waged, and must be won, by the new rules of the Information Age. Data and knowledge are the strategic elements of power. With just a few keystrokes, individuals and groups can now acquire technologies and capabilities once the sole province of nation-states. Modern, adaptable networks asymmetrically attack the rigid, hierarchical structures of the past.

In this environment, there is security in sharing, not hording, information that many more people need to know. We asked our witnesses this afternoon to help us assess the impact of current access restrictions on efforts to create the trusted networks and new information sharing pathways critical to our national security. We look forward to their testimony.